(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－57112
(P2000－57112A)
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　15/16	６２０	Ｇ０６Ｆ　15/16	６２０Ｂ	５Ｂ０４５
13/00	３５１	13/00	３５１Ｚ	５Ｂ０８９
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ａ	５Ｊ１０４
	６６０		６６０Ｅ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ	

審査請求　未請求　請求項の数22　ＯＬ　（全 18 頁）

(21)出願番号　特願平10－226430

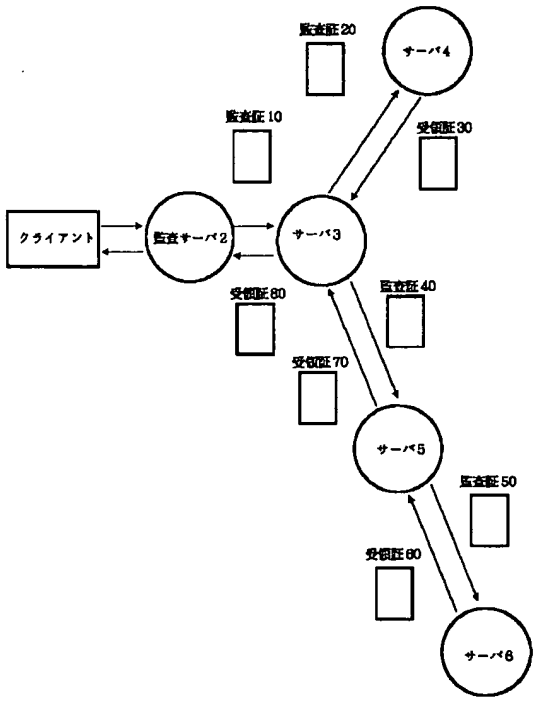
(22)出願日　平成10年８月11日(1998.8.11)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　堀切　和典
神奈川県足柄上郡中井町境430グリーンテクなかい　富士ゼロックス株式会社
(74)代理人　100086531
弁理士　澤田　俊夫

Ｆターム(参考)　5B045 GG06 JJ33 JJ35 KK03
5B089 GA11 GA19 GB09 KA17 KC47
KC53 KC58 KH30
5J104 AA07 KA01 PA07

(54)【発明の名称】　ネットワーク上で遠隔手続き呼び出しを実行するための方法、及び、遠隔手続き呼び出しを実行可能なネットワーク・システム

(57)【要約】
【課題】　サービス要求の出所を認証したり、サーバから提供されたサービスを保証することができる遠隔手続き呼び出し方式を提供する。
【解決手段】　中継サーバは、クライアントからの要求メッセージを受信すると、これに署名を付けてサーバに送信する。サーバは、中継サーバを認証してサービス要求の出所を確認するとともに、応答メッセージには署名を付けて、中継サーバに応答メッセージを送信する。中継サーバは、署名を認証して、さらに、応答メッセージが正当かどうか検査してから、要求元クライアントに送信する。また、中継サーバは、メッセージの送受信の履歴を記録し、ネットワーク上の不信な動作を監視する。



1

【特許請求の範囲】

【請求項１】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）中継・監査サーバが、クライアントからの第１の要求メッセージを受信するステップと、（ｂ）前記中継・監査サーバが、第１の要求メッセージの要求先である第１のサーバに対して第２の要求メッセージを送信するステップと、（ｃ）前記第１のサーバが、受信した第２の要求メッセージを受信するとともに、第２の要求メッセージが前記中継・監査サーバを経由したことを検査するステップと、（ｄ）前記第１のサーバが、第２の要求メッセージに応答した第１の応答メッセージを前記中継・監査サーバに送信するステップと、（ｅ）前記中継・監査サーバが、受信した第１の応答メッセージが正当なメッセージであることを検査するステップと、（ｆ）前記中継・監査サーバが、第２の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項２】前記第１のサーバは、さらに、前記第２の要求メッセージの少なくとも一部の処理を委ねた第３の要求メッセージを第２のサーバに送信するとともに、前記第２のサーバから受信した応答メッセージとともに前記第１の応答メッセージを前記中継・監査サーバに送信する、ことを特徴とする請求項１に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項３】前記ステップ（ｃ）における検査が異常であれば、前記第１のサーバは受信した第２の要求メッセージの処理を実行しないことを特徴とする請求項１又は２のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項４】前記ステップ（ｅ）における検査が異常であれば、前記中継・監査サーバは第２の応答メッセージを前記クライアントに送信しないことを特徴とする請求項１又は２のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項５】さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含むことを特徴とする請求項１又は２のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項６】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）中継・監査サーバが、クライアントからの第１の要求メッセージを受信するとともに、ユーザを特定するステップと、（ｂ）前記中継・監査サーバが、第１の要求メッセージの要求先である第１のサーバに対して第２の要求メッセージを送信するステップと、（ｃ）前記第１のサーバが、受信した第２の要求メッセージを受信するとともに、前記中継・監査サーバからのメッセージであることを特定するステップと、（ｄ）前記第１のサーバが、第２の要求メッセージに応答した第１の応答メッセージを前記中継・監査サーバに送信するステップと、（ｅ）前記中継・監査サーバが、受信した第１の応答メッセージが正当なメッセージであることを検査するステップと、（ｆ）前記中継・監査サーバが、第２の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法。

2

【請求項７】前記第１のサーバは、さらに、前記第２の要求メッセージの少なくとも一部の処理を委ねた第３の要求メッセージを第２のサーバに送信するとともに、前記第２のサーバから受信した応答メッセージとともに第１の応答メッセージを前記中継・監査サーバに送信する、ことを特徴とする請求項６に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項８】前記ステップ（ｅ）における検査が異常であれば、前記中継・監査サーバは第２の応答メッセージを前記クライアントに送信しないことを特徴とする請求項６又は７のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項９】さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含むことを特徴とする請求項６又は７のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項１０】サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）中継・監査サーバが、クライアントからの第１の要求メッセージを受信するステップと、（ｂ）前記中継・監査サーバが、第１の要求メッセージの要求先である第１のサーバに対して、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けた第２の要求メッセージを送信するステップと、

（ｃ）前記第１のサーバが、受信した第２の要求メッセージを受信するとともに、前記中継・監査サーバの公開鍵を用いて認証するステップと、（ｄ）前記第１のサーバが、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、第２の要求メッセージに応答した第１の応答メッセージを前記中継・監査サーバに送信するステップと、（ｅ）前記中継・監査サーバが、第１の応答メッセージを受信し、前記第１のサーバの公開鍵を用いて認証するとともに、正当なメッセージであることを検査するステップと、（ｆ）前記中継・監査サーバが、第２の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔

手続き呼び出しを実行するための方法。

【請求項１１】前記第１のサーバは、さらに、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、前記第２の要求メッセージの少なくとも一部の処理を委ねた第３の要求メッセージを第２のサーバに送信し、

前記第２のサーバは、前記第２のメッセージを受信して、前記第１のサーバの公開鍵を用いて認証するとともに、これに応答した応答メッセージを自身の公開鍵暗号系の秘密鍵を用いた署名を付けて前記第１のサーバに送信し、

前記第１のサーバは、受信した応答メッセージを前記第２のサーバの公開鍵を用いて認証した後に、第１の応答メッセージを前記中継・監査サーバに送信する、ことを特徴とする請求項１０に記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項１２】前記ステップ（ｃ）における認証が異常であれば、前記第１のサーバは受信した第２の要求メッセージの処理を実行しないことを特徴とする請求項１０又は１１のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項１３】前記ステップ（ｅ）における認証が異常であれば、前記中継・監査サーバは第２の応答メッセージを前記クライアントに送信しないことを特徴とする請求項１０又は１１のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項１４】さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含むことを特徴とする請求項１０又は１１のいずれかに記載のネットワーク上で遠隔手続き呼び出しを実行するための方法。

【請求項１５】遠隔手続き呼び出しが実行可能なネットワーク・システムであって、

サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、

サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、１以上の中継・監査サーバと、

サービス要求メッセージを受信して、正当な経路を介して受信したメッセージであることを検査するとともに、要求されたメッセージに応答した応答メッセージを送信する、サービス・オブジェクトを有する１以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項１６】遠隔手続き呼び出しが実行可能なネットワーク・システムであって、

サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、

サービス要求メッセージを受信し、その要求元を特定してから要求先のサーバに向けて転送するとともに、受信

したサービス応答メッセージを要求元のクライアントに向けて転送する、１以上の中継・監査サーバと、

サービス要求メッセージを受信して、メッセージの送信元を特定するとともに、要求されたメッセージに応答した応答メッセージを送信する、サービス・オブジェクトを有する１以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項１７】遠隔手続き呼び出しが実行可能なネットワーク・システムであって、

サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、

サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、サービス要求に対する応答メッセージを受信して、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、１以上の中継・監査サーバと、

サービス要求メッセージを受信して、要求されたメッセージに応答した応答メッセージを送信する、サービス・オブジェクトを有する１以上のサーバとを具備し、

前記中継・監査サーバ及びサーバは、メッセージ送信時には自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付け、メッセージ受信時には送信元の公開鍵を用いて認証を行うことを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項１８】前記中継・監査サーバは、受信したサービス応答メッセージが正当なメッセージであることを検査してからサービスの要求元に向けて送信するとともに、要求メッセージ及び／又は応答メッセージの送受信の履歴を記録することを特徴とする請求項１５乃至１７のいずれかに記載の遠隔手続き呼び出しが実行可能なネットワーク・システム。

【請求項１９】サービスを要求する１以上のクライアントと要求されたサービスを提供する１以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、

サービス要求メッセージを受信する手段と、

自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、

サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、を具備することを特徴とするサーバ。

【請求項２０】サービスを要求する１以上のクライアントと要求されたサービスを提供する１以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、

サービス要求メッセージを受信するとともにその要求元

5

を特定する手段と、
自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、
サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、
を具備することを特徴とするサーバ。を特徴とするサーバ。
【請求項２１】さらに、
受信したサービス応答メッセージが正当なメッセージであることを検査する手段と、
要求メッセージ及び／又は応答メッセージの送受信の履歴を記録する手段と、を含むことを特徴とする請求項１９又は２０のいずれかに記載のサーバ。
【請求項２２】サービスを要求する１以上のクライアントと要求されたサービスを提供する１以上のサーバとで構成されるネットワーク上において実行される遠隔手続き呼び出し動作をサポートする中継・監視サーバであって、
要求メッセージや応答メッセージの送受信を行う送受信部と、
受信した要求メッセージを解析して要求パラメータを抽出する要求メッセージ解析部と、
要求パラメータに所定の情報を連結して電子署名する監査証生成部と、
応答メッセージを解析して、送信元のサーバが電子署名した受領証を抽出する応答メッセージ解析部と、
受領証を電子認証する受領証処理部と、を含むことを特徴とする中継・監視サーバ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、１以上のサーバと１以上のクライアントからなる分散環境のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための遠隔手続き／メソッド呼び出し方式に係り、特に、少なくとも１つの中継・監査サーバを中継してサービスの要求がサーバに届くようなタイプの遠隔手続き呼び出し／メソッド方式に関する。
【０００２】更に詳しくは、本発明は、クライアントが要求するサービスを複数のサーバの協働的な動作によって提供するような分散型のネットワーク環境において、遠隔的に要求されたサービスの履行を保証するための方式に係り、特に、ネットワーク上に中継・監査サーバを介在させることで、サービス要求の出所を認証したり、サーバから提供されたサービスの品質等を保証することができる遠隔手続き呼び出し／メソッド方式に関する。
【０００３】
【従来の技術】昨今の情報処理・情報通信の分野における発展は目覚しいものがある。この種の技術分野においては、コンピュータ・システム同士を相互接続するため

6

の研究・開発が、従来より活発になされてきた。システム同士を相互接続する主な目的は、複数ユーザによるコンピュータ資源の共有や、情報の共有・流通などである。
【０００４】システム間を接続するための伝送媒体すなわち「ネットワーク」としては、大学や事業所の構内など限られた空間内に敷設されたＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）の他、ＬＡＮを専用回線で接続したＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）や、一般公衆回線（ＰＳＴＮ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、インターネットなど様々である。
【０００５】ＬＡＮは、一般に、ネットワーク上の特定のコンピュータをサーバ（ファイル・サーバ，プリント・サーバ）とし、これを他のクライアントが利用し合うというクライアント・サーバ型として構築される。かかるクライアント・サーバ・モデルでは、プログラムの一部の手続きの実行をネットワーク上の別のコンピュータに委託するというメカニズム、すなわち「遠隔手続き呼び出し（ＲＰＣ：Ｒｅｍｏｔｅ Ｐｒｏｃｅｄｕｒｅ Ｃａｌｌ）」、若しくは「遠隔メソッド呼び出し（ＲＭＩ：Ｒｅｍｏｔｅ Ｍｅｔｈｏｄ Ｉｎｖｏｃａｔｉｏｎ）」が用いられる。遠隔手続きの実行結果は、戻り値として、呼び出した側のコンピュータに返される。また、手許のコンピュータのキーボードやファイルを使ってプログラムへの入力を果たしたり、同じコンピュータのディスプレイやファイルに出力することもできる。
【０００６】遠隔手続き若しくは遠隔メソッド呼び出しの仕組みは、ＬＡＮの世界に限定されず、さらに、インターネットのような広域的なネットワーク上でも利用可能である。インターネット上で利用可能な各種プロトコル、例えば、ＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ），ＨＴＴＰＳ，Ｓ－ＨＴＴＰ（ｓｅｃｕｒｅ ＨＴＴＰ），ＦＴＰ（Ｆｉｌｅ ＴｒａｎｓｆｅｒＰｒｏｔｏｃｏｌ），ＣＯＲＢＡ（Ｃｏｍｍｏｎ ＯＲＢ Ａｒｃｈｉｔｅｃｔｕｒｅ），ＩＩＯＰ（Ｉｎｔｅｒｎｅｔ Ｉｎｔｅｒ－ＯＲＢ Ｐｒｏｔｏｃｏｌ），ＪａｖａＲＭＩ（Ｒｅｍｏｔｅ Ｍｅｔｈｏｄ Ｉｎｖｏｃａｔｉｏｎ）なども、遠隔手続き／遠隔メソッド呼び出しとして実現される。インターネットの代表的なクライアント・サーバ・モデルは、ＷＷＷ（Ｗｏｒｌｄ ＷｉｄｅＷｅｂ）サーバとＷＷＷブラウザとで構成される（周知）。
【０００７】ＷＷＷサーバは、通常、多数のサービス・オブジェクトを蓄積しており、ＷＷＷクライアントからのサービス要求に応答して、インターネット経由でサービスを提供している。サービス・オブジェクトの一例は、ＷＷＷクライアント（ブラウザ）のディスプレイ上においてホームページを形成するためのＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）

ファイルである。WWWサーバが持つ各サービス・オブジェクトの所在は、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）という形式で表される。ＵＲＬは、インターネット上の各種情報リソースにアクセスする手段（すなわち通信プロトコル）とリソースの名前を指定する形式、すなわち「プロトコル名：／／サーバ名（／ディレクトリ名…）／ファイル名」という形式で記述される。

【０００８】WWWクライアントとしてのブラウザは、WWWサーバに対して、ＵＲＬに基づいた形式のサービス要求メッセージを送信する。他方、WWWサーバは、サービス要求メッセージを解釈して、要求されたサービスを提供する。但し、サーバは、要求されたサービスをサーバ単体で実行するとは限らず、さらに別のサーバにサービスの一部の提供を委ねることもある。サーバが他のサーバにサービスの提供を要求する方式の１つはＣＧＩ（Ｃｏｍｍｏｎ　Ｇａｔｅｗａｙ　Ｉｎｔｅｒｆａｃｅ）である（ＣＧＩは、それ自体が標準規約となっているため、この規約を遵守しさえすれば、Ｖｉｓｕａｌ　Ｂａｓｉｃ，Ｃ，Ｄｅｌｐｈｉ，Ｐｅｒｌなど各種言語でＣＧＩプログラムを作成することができる）。

【０００９】例えば、WWWクライアントがブラウザ画面上で検索項目を入力したときは、WWWサーバは、検索の実行と検索結果の送信を他のデータベース・サーバに要求することがある。この場合、データベース・サーバは、ＣＧＩなどの仕組みによってWWWサーバに連動して、要求されたサービスの一部を提供する。データベース・サーバは、検索結果を示すテーブル中の該当するカラムの内容を生成し、WWWサーバはテーブルの残りの部分を生成する（図６参照のこと）。

【００１０】クライアントからのサービス要求を第１に受け取ったサーバ（仮に「親サーバ」とする）は、ホームページ内の一部のコンテンツの生成を別のサーバ（仮に「子サーバ」とする）に委ねる。そして、親サーバは、自身が生成したコンテンツと子サーバから戻されたコンテンツとからホームページを生成して、クライアントに戻すという訳である。さらに子サーバは自分の子サーバ（「孫サーバ」）にサービスの一部の提供を委ねることもある。

【００１１】サービスを提供する複数のサーバの親子関係は、一種の木構造を形成する。図７にはこれを模式的に示している。同図において、サーバＢは、クライアントからのサービス要求（ＵＲＬ）を最初に受け取る親サーバであり、サーバＡとＣはサーバＢの子サーバである。さらに、サーバＣから一部のサービスの提供を要求されるサーバＤは、サーバＢの孫サーバである。

【００１２】従来、殆どの場合において、クライアントから要求されたサービスを実行するサーバ、すなわち木構造を構成する各サーバは、全て単一若しくは同系統の団体に所属し、互いの利益は略一致していた（例えば図６では、データベース・サーバは、WWWサーバと同じ「組織１」に属している）。クライアントが要求したサービスは物理的には複数のサーバの協働的な動作によって提供されるが、クライアントの立場からすれば、このような木構造の仕組みを意識する必要がなく、実質上１つのサーバが責任を持ってサービスを提供すると思うことができた。言い換えれば、クライアントは、サービスの要求先のサーバを信頼するだけで充分だった訳である。

【００１３】ところが、コンピュータ・ネットワーキングの世界がさらに進化を遂げるに従い、ネットワークを構成する各マシン間の関係も高度に複雑化してくる。例えば、ある特定のサービスを提供するためのサーバの木構造は、別個の団体に跨ったサーバの集合で構成されることもあり得る。例えば図７では、サーバＢとデータベース・サーバは「組織１」に所属するが、子サーバＡは「組織２」に、子サーバＣと孫サーバＤは「組織３」に所属している。親サーバＢと子サーバＣとが、異なる団体に所属して両者の利害が完全には一致しない、ということも予想される。

【００１４】あるクライアントが有料でサーバＢへのアカウントを取得したような場合、クライアントは、サーバＢを全面的に信用するであろうし、サーバＢも受け取ったアカウント料金に見合ったサービスを提供するよう努め、また、信用を裏切ることを敢えてしないであろう。しかしながら、別団体のサーバＣは、クライアントに対して何の義務も義理も感じることはなく、或いはクライアントに対し悪意を抱き、正当なサービスの提供を拒否し或いは不当なサービスを行うという可能性もある。サーバＢが子サーバＣからの不当なサービスをそのままクライアントに戻したならば、クライアントは大きな打撃を被り、あるいは壊滅しかねない。現状のネットワーク環境において、クライアントに戻されるサービスを保証するようなメカニズムはない。

【００１５】また、子サーバＣが親サーバＢとは異なる団体に所属するような場合、サーバＢがサーバＣに対してサービス提供の対価を支払うような、一種の契約関係が成立していることもある。この対価の額が従量制、すなわちクライアントからのサービス要求の回数に応じて定まることもある。このような場合、サーバＣは、サーバＢに対するダミーのサービス要求を頻繁に発行せしめることによって、対価額すなわち利益を貪ることもできる（図８を参照のこと）。ダミーのサービス要求は、一般ユーザを装った不正クライアントによって容易に発行される。現状のネットワーク環境において、サーバＢが、サーバＣやダミー・クライアントのような不正行為を取り締まるようなメカニズムはない。

【００１６】

【発明が解決しようとする課題】本発明の目的は、１以上のサーバと１以上のクライアントからなる分散型のネ

ットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための、優れた遠隔手続き呼び出しを行う方式を提供することにある。

【００１７】本発明の更なる目的は、少なくとも１つの中継・監査サーバを中継してサービスの要求がサーバに届くようなタイプの、優れた遠隔手続き呼び出し方式を提供することにある。

【００１８】本発明の更なる目的は、クライアントから要求されたサービスを複数のサーバの協働的な動作によって提供するような分散型のネットワーク環境において、サービスの正当な履行を保証するための優れた方式を提供することにある。

【００１９】本発明の更なる目的は、ネットワーク上に中継・監査サーバを配設することで、サービス要求の出所を認証したり、サーバから提供されたサービスの品質等を保証することができる、優れた遠隔手続き呼び出し方式を提供することにある。

【００２０】

【課題を解決するための手段】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）中継・監査サーバが、クライアントからの第１の要求メッセージを受信するステップと、（ｂ）前記中継・監査サーバが、第１の要求メッセージの要求先である第１のサーバに対して第２の要求メッセージを送信するステップと、（ｃ）前記第１のサーバが、受信した第２の要求メッセージを受信するとともに、第２の要求メッセージが前記中継・監査サーバを経由したことを検査するステップと、（ｄ）前記第１のサーバが、第２の要求メッセージに応答した第１の応答メッセージを前記中継・監査サーバに送信するステップと、（ｅ）前記中継・監査サーバが、受信した第１の応答メッセージが正当なメッセージであることを検査するステップと、（ｆ）前記中継・監査サーバが、第２の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【００２１】ここで、前記第１のサーバは、さらに、前記第２の要求メッセージの少なくとも一部の処理を委ねた第３の要求メッセージを第２のサーバに送信するとともに、前記第２のサーバから受信した応答メッセージとともに第１の応答メッセージを前記中継・監査サーバに送信するようにしてもよい。

【００２２】また、前記ステップ（ｃ）における検査が異常であれば、前記第１のサーバは受信した第２の要求メッセージの処理を実行しないようにしてもよい。

【００２３】また、前記ステップ（ｅ）における検査が異常であれば、前記中継・監査サーバは第２の応答メッセージを前記クライアントに送信しないようにしてもよい。

【００２４】また、さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含んでいてもよい。

【００２５】また、本発明の第２の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）中継・監査サーバが、クライアントからの第１の要求メッセージを受信するとともに、ユーザを特定するステップと、（ｂ）前記中継・監査サーバが、第１の要求メッセージの要求先である第１のサーバに対して第２の要求メッセージを送信するステップと、（ｃ）前記第１のサーバが、受信した第２の要求メッセージを受信するとともに、前記中継・監査サーバからのメッセージであるしたことを特定するステップと、（ｄ）前記第１のサーバが、第２の要求メッセージに応答した第１の応答メッセージを前記中継・監査サーバに送信するステップと、（ｅ）前記中継・監査サーバが、受信した第１の応答メッセージが正当なメッセージであることを検査するステップと、（ｆ）前記中継・監査サーバが、第２の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【００２６】ここで、前記第１のサーバは、さらに、前記第２の要求メッセージの少なくとも一部の処理を委ねた第３の要求メッセージを第２のサーバに送信するとともに、前記第２のサーバから受信した応答メッセージとともに第１の応答メッセージを前記中継・監査サーバに送信するようにしてもよい。

【００２７】また、前記ステップ（ｅ）における検査が異常であれば、前記中継・監査サーバは第２の応答メッセージを前記クライアントに送信しないようにしてもよい。

【００２８】また、さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含んでもよい。

【００２９】また、本発明の第３の側面は、サービスを要求する１以上のクライアントとサービス・オブジェクトを有する１以上のサーバとで構成されるネットワーク上において遠隔手続き呼び出しを実行するための方法であって、（ａ）中継・監査サーバが、クライアントからの第１の要求メッセージを受信するステップと、（ｂ）前記中継・監査サーバが、第１の要求メッセージの要求先である第１のサーバに対して、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けた第２の要求メッセージを送信するステップと、（ｃ）前記第１のサーバが、受信した第２の要求メッセージを受信するとともに、前記

中継・監査サーバの公開鍵を用いて認証するステップと、（ｄ）前記第１のサーバが、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、第２の要求メッセージに応答した第１の応答メッセージを前記中継・監査サーバに送信するステップと、（ｅ）前記中継・監査サーバが、第１の応答メッセージを受信し、前記第１のサーバの公開鍵を用いて認証するとともに、正当なメッセージであることを検査するステップと、（ｆ）前記中継・監査サーバが、第２の応答メッセージを前記クライアントに送信するステップと、を具備することを特徴とするネットワーク上で遠隔手続き呼び出しを実行するための方法である。

【００３０】ここで、前記第１のサーバは、さらに、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、前記第２の要求メッセージの少なくとも一部の処理を委ねた第３の要求メッセージを第２のサーバに送信し、前記第２のサーバは、前記第２のメッセージを受信して、前記第１のサーバの公開鍵を用いて認証するとともに、これに応答した応答メッセージを自身の公開鍵暗号系の秘密鍵を用いた署名を付けて前記第１のサーバに送信し、前記第１のサーバは、受信した応答メッセージを前記第２のサーバの公開鍵を用いて認証した後に、第１の応答メッセージを前記中継・監査サーバに送信する、ようにしてもよい。

【００３１】また、前記ステップ（ｃ）における認証が異常であれば、前記第１のサーバは受信した第２の要求メッセージの処理を実行しないようにしてもよい。

【００３２】また、前記ステップ（ｅ）における認証が異常であれば、前記中継・監査サーバは第２の応答メッセージを前記クライアントに送信しないようにしてもよい。

【００３３】また、さらに、前記中継・監査サーバが要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するステップを含んでもよい。

【００３４】また、本発明の第４の側面は、遠隔手続き呼び出しが実行可能なネットワーク・システムであって、サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、１以上の中継・監査サーバと、サービス要求メッセージを受信し、正当な経路を介して受信したメッセージであることを検査するとともに、要求されたメッセージに応答した応答メッセージを送信する、サービス・オブジェクトを有する１以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システムである。

【００３５】また、本発明の第５の側面は、遠隔手続き呼び出しが実行可能なネットワーク・システムであって、サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信し、その要求元を特定してから要求先のサーバに向けて転送するとともに、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、１以上の中継・監査サーバと、サービス要求メッセージを受信して、メッセージの送信元を特定するとともに、要求されたメッセージに応答した応答メッセージを送信する、サービス・オブジェクトを有する１以上のサーバと、を具備することを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システムである。

【００３６】また、本発明の第６の側面は、遠隔手続き呼び出しが実行可能なネットワーク・システムであって、サービスを要求する要求メッセージを送信するとともにその応答メッセージを受信するクライアントと、サービス要求メッセージを受信して要求先のサーバに向けて転送するとともに、サービス要求に対する応答メッセージを受信して、受信したサービス応答メッセージを要求元のクライアントに向けて転送する、１以上の中継・監査サーバと、サービス要求メッセージを受信して、要求されたメッセージに応答した応答メッセージを送信する、サービス・オブジェクトを有する１以上のサーバとを具備し、前記中継・監査サーバ及びサーバは、メッセージ送信時には自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付け、メッセージ受信時には送信元の公開鍵を用いて認証を行うことを特徴とする遠隔手続き呼び出しが実行可能なネットワーク・システムである。

【００３７】本発明の上記第４乃至第６の側面に係るネットワーク・システムにおいて、前記中継・監査サーバは、受信したサービス応答メッセージが正当なメッセージであることを検査してから要求元に向けて送信するとともに、要求メッセージ及び／又は応答メッセージの送受信の履歴を記録するようにしてもよい。

【００３８】また、本発明の第７の側面は、サービスを要求する１以上のクライアントと要求されたサービスを提供する１以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、サービス要求メッセージを受信する手段と、自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、を具備することを特徴とするサーバである。

【００３９】また、本発明の第８の側面は、サービスを要求する１以上のクライアントと要求されたサービスを提供する１以上のサーバとで構成されるネットワーク上において、サービス要求メッセージやサービス応答メッセージを受信し或いは送信するサーバであって、サービ

ス要求メッセージを受信するとともにその要求元を特定する手段と、自身の署名を付けてサービス要求メッセージをさらに別のサーバに向けて送信する手段と、サービス要求に対する応答メッセージを受信して、送信元を認証してからサービス要求元のクライアントに向けて送信する手段と、を具備することを特徴とするサーバ。を特徴とするサーバである。

【００４０】本発明の上記第７及び第８の側面に係るサーバにおいて、さらに、受信したサービス応答メッセージが正当なメッセージであることを検査する手段と、要求メッセージ及び／又は応答メッセージの送受信の履歴を記録する手段と、を含んでいてもよい。

【００４１】また、本発明の第９の側面は、サービスを要求する１以上のクライアントと要求されたサービスを提供する１以上のサーバとで構成されるネットワーク上において実行される遠隔手続き呼び出し動作をサポートする中継・監視サーバであって、要求メッセージや応答メッセージの送受信を行う送受信部と、受信した要求メッセージを解析して要求パラメータを抽出する要求メッセージ解析部と、要求パラメータに所定の情報を連結して電子署名する監査証生成部と、応答メッセージを解析して、送信元のサーバが電子署名した受領証を抽出する応答メッセージ解析部と、受領証を電子認証する受領証処理部と、を含むことを特徴とする中継・監視サーバである。

【００４２】

【作用】本発明に係る分散型のネットワーク・システムには、サービスを要求する１以上のクライアントと、サービス・オブジェクトを有する１以上のサーバが存在する。

【００４３】サーバは、ある１つのサービス要求に対して、自身が所有するサービス・オブジェクトのみを以って応答してもよいが、他のサーバとの協働的動作によって応答しても良い。サーバ同士は、例えばＣＧＩ（Ｃｏｍｍｏｎ　ＧａｔｅｗａｙＩｎｔｅｒｆａｃｅ）のような接続形態によって協働的動作を実現することができる。

【００４４】本発明においては、サービスを要求するクライアントは、サービス・オブジェクトを有するサーバに直接アクセスすることはせずに、中継・監査サーバに対してサービス要求メッセージを送信する。この中継・監査サーバは、ネットワーク・システム上のいずれかの場所に配設されているものとする。

【００４５】ネットワーク・システムがインターネットであれば、サーバは例えば無数のＨＴＭＬ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ファイルを所有するＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）サーバであり、サービス・オブジェクトはＨＴＭＬＴファイル（ホームページ）である。また、クライアントはＵＲＬ（Ｕｎｉｆｏｒｍ　ＲｅｓｏｕｒｃｅＬｏｃａｔｏｒ）の送信という形態でサービス要求メッセージを送信することができる。

【００４６】中継・監査サーバは、クライアントからの要求メッセージを受信すると、この受信メッセージに自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、該当するサービス・オブジェクトを持つサーバに向けて送信する。ここで、中継・監査サーバは、要求メッセージを中継する際に、サービスの要求元であるクライアント・ユーザを特定してもよい。特定することによって、中継・監査サーバは、要求メッセージの出所を証明したり、受信ログを記録することができる。また、中継・監査サーバはメッセージの送信ログを記録してもよい。

【００４７】サービス・オブジェクトを持つサーバは、中継・監査サーバを介して要求メッセージを受け取ると、中継・監査サーバの公開鍵を用いて認証し、サービス要求の出所を確認することができる。認証を行うことによって、サーバは安心してサービスを提供することができる。

【００４８】サーバは、自身が所有するサービス・オブジェクトのみを以って要求メッセージに応答する。この場合は、自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、中継・監査サーバに応答メッセージを送信する。

【００４９】あるいは、サーバは、要求されたサービスの処理の一部を他のサーバ（例えば木構造を形成する子サーバ）に委ねることができる。この場合、サーバは自身が持つ公開鍵暗号系の秘密鍵を用いた署名を付けて、要求メッセージを他のサーバに送信する。

【００５０】サーバから要求メッセージを受け取った他のサーバ（子サーバ）は、公開鍵を用いて要求元のサーバを認証する。そして、応答メッセージを戻すときには、自身の公開鍵暗号系の秘密鍵を用いた署名を行う。他のサーバは、さらに他のサーバ（孫サーバ）にサービスを要求することもできるが、この場合は同様に、要求メッセージ送信時における署名と応答メッセージ受信時における認証を伴う。

【００５１】サーバが要求サービスに応答した応答メッセージは、クライアントに戻される前に、一旦、中継・監査サーバにて受信される。この応答メッセージには、サーバの署名が付加されている。応答メッセージが複数のサーバの連携によって形成されているときには、これに関わった全て（又は少なくとも一部）のサーバの署名が応答メッセージに付加されている。中継・監査サーバは、各サーバの公開鍵を用いて署名を認証して、サービス・オブジェクトの出所を確認する。さらに、中継・監査サーバは、応答メッセージの中身がサービス要求に対する正当なメッセージであるかどうか検査する。応答メッセージの内容が異常若しくは不当なものであれば、例えば再送要求を発行したり警告を発したりしてもよい。

【００５２】このような認証や検査工程を経て、応答メッセージが中継・監査サーバから要求元クライアントに送信される。応答メッセージはその出所が明らかであり、内容も検査済みであるから、クライアントは信頼してこれを受理することができる。

【００５３】また、中継・監査サーバは、要求メッセージや応答メッセージの送受信の履歴を記録し、遠隔手続き呼び出し動作を監視することができる。例えば、要求元のクライアントが同じサービス要求を頻繁に発行しているなど、ある特定のクライアント・ユーザがネットワーク上で不信な挙動を行っているときには、要求先のサーバ側に通知したりクライアントに警告を発したりしてもよい。

【００５４】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５５】

【発明の実施の形態】以下、図面を参照しながら本発明の実施例を詳解する。

【００５６】図１には、本発明の実施に供されるネットワーク・システム１００の構成を模式的に示している。ネットワーク・システム１００は、データ（すなわちサービス要求メッセージやサービス応答メッセージなど）の伝送媒体であるネットワーク１０に無数のデータ端末装置５０Ａ，５０Ｂ…が接続されており、分散コンピューティング環境を提供している。以下、各部について説明する。

【００５７】ネットワーク１０は、例えば大学や企業の構内などの限られた空間内に敷設されたＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）である。あるいは、ＬＡＮ同士を専用線等で相互接続してなるＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）や、一般公衆回線（ＰＳＴＮ：Ｐｕｂｌｉｃ Ｓｗｉｔｃｈｅｄ Ｔｅｌｅｐｈｏｎｅ Ｎｅｔｗｏｒｋ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、これらネットワークの大規模な集合体であるインターネットであってもよい。各データ端末装置５０Ａ…は、モデムやＴＡ（Ｔｅｒｍｉｎａｌ Ａｄａｐｔｅｒ）、ＬＡＮアダプタ等を介してネットワーク１０に接続される。

【００５８】データ端末装置５０Ａ…の一部はサービスを提供するサーバであり、その他はサービスを要求するクライアントである。データ端末装置５０Ａ…は、サーバ或いはクライアントとしてデザインされた専用のマシンであってもよいが、多くの場合は、サーバ用又はクライアント用のアプリケーションを導入して動作する汎用のコンピュータ・システムである。各データ端末装置同士は、ネットワーク１０を介して、例えばＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ ＣｏｎｔｒｏｌＰｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）接続されている。

【００５９】サーバは、複数のサービス・オブジェクトを所有しており、サービス要求に応じて適宜サービス・オブジェクトを要求元に提供する。サービス・オブジェクトの一例は、ホームページを形成するためのＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）ファイルであり、ＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）プロトコルに従ってネットワーク１０経由で伝送することができる。また、クライアントは、ＵＲＬの形式に従って所望のサービス・オブジェクトを指定することができる。

【００６０】ネットワーク１０を介したＵＲＬによるサービス要求は、一種の遠隔手続き／メソッド呼び出しである。また、サーバは、ある１つのサービス要求に対して、自分一人で実行するとは限らず、さらに別のサーバにサービスの一部の提供を委ねることもある。サーバが他のサーバにサービスの提供を要求する方式の１つはＣＧＩ（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ）である。すなわち、クライアントからのサービス要求を第１に受け取ったサーバ（仮に「親サーバ」とする）は、ホームページ内におけるコンテンツの一部の生成を別のサーバ（仮に「子サーバ」とする）に委ねる。そして、親サーバは、自ら生成したコンテンツと子サーバから戻されたコンテンツとからホームページを生成して、クライアントに戻すという仕組みである。さらに子サーバは自分の子サーバ（「孫サーバ」）にサービスの一部の提供を委ねることもある。サービスを提供する複数のサーバの親子関係は、一種の木構造を形成する。このような場合、要求されたサービスに対する応答は、木構造をなす各サーバ間の協働的な連携作業によって果たされる。

【００６１】例えば、ＷＷＷクライアントがブラウザ画面上で検索項目を入力したときは、ＷＷＷサーバは、検索の実行と検索結果の送信を他のデータベース・サーバに要求することがある。この場合、データベース・サーバは、ＣＧＩなどの仕組みによってＷＷＷサーバに連動して、要求されたサービスの一部を提供する。すなわち、データベース・サーバは、検索結果を示すテーブル中の該当カラムの内容を生成し、ＷＷＷサーバはテーブルの残りの部分を生成する（前述）。

【００６２】本発明において特にユニークなのは、ネットワーク１０上に存在するサーバの少なくとも１つが「中継・監視サーバ」として機能する点である。この中継・監視サーバは、クライアントに代行してサーバにサービス要求を行うようになっている。クライアントは、サーバに直接アクセスせず、中継・監視サーバに対してサービス要求メッセージを送信し、また、中継・監視サーバを経由してサービス応答メッセージを受信する。

【００６３】中継・監視サーバは、メッセージ受信の際には送信元の認証を行うことでメッセージの内容を保証

する。メッセージ送信の際には、自ら署名を行うことで、メッセージの出所証明を行う。クライアントは、中継・監視サーバを介することで、安心してサービスの提供を受けることができる。また、中継・監視サーバは、サービスを要求するクライアント・ユーザを特定したり、そのログを記録することで、ユーザの不信な挙動をも監視する。中継・監視サーバを含んだメッセージ送受信オペレーションの詳細については後述に委ねる。

【００６４】図２には、クライアントからのあるサービスを提供するために形成されたサーバの木構造を模式的に示している。同図では、サービスを提供する親サーバ３には２つの子サーバ４及び５が存在し、さらに子サーバ５を後継する孫サーバ６が存在する。但し、全てのサーバが同一の運営団体に所属しているとは限らない。また、クライアント１とサーバ４の間には、中継・監視サーバ２が介在している。中継・監視サーバ２は、その機能実現のために特化してデザインされたデータ端末装置であってもよいが、中継・監視サーバ用のアプリケーション・プログラムを導入した汎用コンピュータ・システムであってもよい。

【００６５】図３には、本発明を実現する中継・監視サーバ２の構成を模式的に図解したブロック図である。同図に示すように、中継・監視サーバ２は、監査証作成部２１０と、要求メッセージ解析部２２０と、送受信部２３０と、受領証処理部２４０と、応答メッセージ解析部２５０とで構成される。以下、各部について説明する。

【００６６】送受信部２３０は、ネットワーク１０経由でのメッセージの送受信を行うための装置である。クライアント１に対しては、サービス要求メッセージの受信とサービス応答メッセージの送信を行う。また、サーバ３に対しては、サービス要求メッセージの送信と、サービス応答メッセージの受信を行う。

【００６７】要求メッセージ解析部２２０は、送受信部２３０から受け取ったサービス要求メッセージの解析処理を行う。また、要求メッセージ中の要求パラメータを抽出して監査証作成部２１０に渡す。

【００６８】監査証生成部２１０は、電子署名を行うために、公開鍵暗号系の秘密鍵を所有する。要求メッセージ解析部２２０から要求パラメータを渡されると、これに監査証番号とその有効期限を表した文字列を連結して、さらに秘密鍵を用いて電子署名する。この電子署名は、中継・監視サーバ２が発行する監査証を意味する。この後、監査証が付された要求メッセージは、送受信部２３０から送出される。また、監査証生成部２１０は、クライアントからの要求メッセージを管理するためのログ・ファイルを備えており、クライアントからの要求メッセージを処理する度に、ログをとるようになっている。

【００６９】応答メッセージ解析部２５０は、サーバから受信した応答メッセージの解析処理を行う。応答メッセージには、送信元のサーバによって電子署名が施された受領証が含まれている。応答メッセージ解析部２５０は、応答メッセージから受領証を抽出して、受領証処理部２４０に渡す。

【００７０】受領証処理部２４０は、各サーバ３，４，５，６の公開鍵を保持しており、応答メッセージ解析部２５０から渡された受領証の署名の認証を行う。本実施例では、サーバ３から戻されたサービス応答メッセージ中には、サービス応答に携わった全て（又は少なくとも一部）のサーバ３，４，…の電子署名が施されている（後述）。これら電子署名は、各サーバ３，４，…の受領証の役割を持つ。受領証処理部２４０は、該当するサーバの公開鍵を用いて各署名を電子認証する。また、受領証処理部２４０は、各サーバ毎のログ・ファイルを管理しており、認証手続きに成功したときには該当するサーバのログ・ファイルにそのログを追加するようになっている。

【００７１】なお、図３に示した各ブロックは、専用のハードウェア装置としてデザインすることも、或いは汎用コンピュータ・システムに導入されたプログラム・モジュールの形態で実装することも可能である。

【００７２】図４には、本発明の実施に供されるサーバ３の構成を模式的に図解したブロック図である。同図に示すように、サーバ３は、サービス・オブジェクト部３１０と、応答メッセージ生成部３２０と、要求メッセージ解析部３３０と、送受信部３４０と、応答メッセージ解析部３５０と、要求メッセージ生成部３６０とで構成される。以下、各部について説明する。

【００７３】送受信部３４０は、ネットワーク１０経由でのメッセージの送受信を行うための装置である。中継・監査サーバ２若しくは自分の親サーバに対しては、サービス要求メッセージの受信とサービス応答メッセージの送信を行う。また、自分の子サーバに対しては、サービス要求メッセージの送信と、サービス応答メッセージの受信を行う。

【００７４】サービス・オブジェクト部３１０は、サーバ３がサービス要求に応答して提供するサービス・オブジェクトの集合で構成される。サービス・オブジェクトの一例は、WWWクライアントのディスプレイ上においてホームページを形成するためのＨＴＭＬファイルである。サービス・オブジェクト部３１０の実体は、サービス・オブジェクトを格納するディスク型格納装置である。クライアント１や子サーバに対してサービスを要求する親サーバは、所望のサービス・オブジェクトをＵＲＬによって指定することができる。

【００７５】要求メッセージ解析部３３０は、送受信部３４０から受け取ったサービス要求メッセージを解析処理する。ここで言う解析処理は、要求メッセージ中の監査証を抽出して、該メッセージの有効性や正当性などのチェックを行うことである。要求メッセージ解析部３３

０は、既に無効となった監査証の識別子を管理するための無効識別子テーブルも備えている。

【００７６】要求メッセージ解析部３３０は、要求メッセージ送信元の公開鍵を用いて監査証を電子認証するとともに、監査証中の有効期限を検証する。有効期限が消滅していれば、次のステップには進まないので、サービス・オブジェクトの提供は行われない。監査証が有効期限内であれば、次に、監査証の識別子が無効識別子テーブル中にないかどうかを確認する。テーブル中に存在すれば、監査証が既に無効であることを意味するので、次のステップには進まず、この結果としてサービス・オブジェクトの提供は行われない。監査証の識別子が無効識別子テーブル中になければ、該識別子を該テーブル中に追加する。この結果、同一の監査証の流用が禁止されることになる。

【００７７】監査証の検査を終えた後、要求メッセージ解析部３３０は、要求メッセージ中の要求パラメータをサービス・オブジェクト部３１０に渡す。サービス・オブジェクト部３１０は、これに応答して、該当するサービス・オブジェクトを自ら所有するときには、該サービス・オブジェクトを応答メッセージ生成部３２０に供給する。また、該当するサービス・オブジェクトを自らは所有せず、サーバ３の子孫のサーバ４，５…が所有するときには、要求メッセージ生成部３６０に対して子孫サーバ４，５…へのサービス要求メッセージの送信を促す。

【００７８】応答メッセージ生成部３２０は、サービス・オブジェクト部３１０から取り出されたサービス・オブジェクトを基にして、応答メッセージを生成する。また、応答メッセージ生成部３２０は、公開鍵暗号系の秘密鍵を所有しており、応答メッセージに対して電子署名を行うことによって、応答メッセージに受領証を添付する。受領証着きの応答メッセージは送受信部３４０によってサービス要求元に送出される。

【００７９】要求メッセージ生成部３６０は、子孫サーバ４，５…に対して送信するサービス要求メッセージを生成するためのものである。要求メッセージ生成部３６０は、公開鍵暗号系の秘密鍵を所有しており、要求メッセージに対して電子署名を行うことにより要求メッセージに監査証を添付する。監査証付きの要求メッセージは、送受信部３４０によってサービス要求先に送出される。なお、子孫サーバ４，５…へのサービス要求は、例えばＣＧＩ（Ｃｏｍｍｏｎ Ｇａｔｅｗａｙ Ｉｎｔｅｒｆａｃｅ）の形態で行われる。

【００８０】応答メッセージ解析部３５０は、送受信部３４０が受信した子孫サーバ４，５…からの応答メッセージを解析するためのものである。応答メッセージには、サービス要求に応答した全て（又は少なくとも一部）の子孫サーバ４，５…の電子署名を含んだ受領証が添付されている。応答メッセージ解析部３５０は、各子孫サーバ４，５…の公開鍵を用いて受領証を電子認証する。また、子孫サーバ４，５…から送られてきたサービス・オブジェクトに加えて、サーバ３自身が所有するサービス・オブジェクトを送るときには、サービス・オブジェクト部３１０に対して所望のサービス・オブジェクトの取り出しを促す（例えば、サーバ３がホームページ上のテーブルを作成し、該テーブル中の所定のカラムを子孫サーバ（データベース・サーバなど）が作成する場合がこれに該当する）。

【００８１】以下でも詳解するが、サーバ３は、サービス・オブジェクトを提供するサーバそのものとして機能する以外に、自分の子孫にあたる各サーバ４，５，６からの応答メッセージを認証する認証局としての役割も持つ、という点を充分理解されたい。

【００８２】なお、図４に示した各ブロックは、専用のハードウェア装置としてデザインすることも、或いは汎用コンピュータ・システムに導入されたプログラム・モジュールの形態で実装することも可能である。

【００８３】また、サーバ３の子孫にあたるその他のサーバ４，５，６も、図４に示したものと同様の構成を具備するものと理解されたい。例えば、図示しないサーバ４は、サービス・オブジェクト部４１０と、応答メッセージ生成部４２０と、要求メッセージ解析部４３０と、送受信部４４０と、応答メッセージ解析部４５０と、要求メッセージ生成部４６０とで構成される。

【００８４】次いで、ネットワーク・システム１００上における遠隔手続き呼び出しの処理動作について説明する。図５には、クライアント１が発行したサービス要求が中継・監視サーバ２及び各サーバ３，４，５…の協働的動作によって処理される様子を模式的に示している。

【００８５】この例では、各サーバ３，４，５…はＨＴＴＰサーバであり、クライアント１はＨＴＴＰプロトコルを用いてサービス要求メッセージを送信するものとする。また、サーバ３は、自分の子孫サーバ４，５…と連携して、ＨＴＭＬで記述された１つのファイルを生成するものとする。例えば、サーバ３がＨＴＭＬファイルに含まれるテーブルの前半部分に該当するサービス・オブジェクトを提供し、その子サーバ４がテーブルの後半部分に該当するサービス・オブジェクトを提供する。サーバ３，４，５…同士は、例えばＣＧＩ（Ｃｏｍｍｏｎ ＧａｔｅｗａｙＩｎｔｅｒｆａｃｅ）に従った手順によって接続される。ここでは、各々のサーバ３，４，５…のドメイン名を仮に”ｓｅｒｖｅｒ３００”，”ｓｅｒｖｅｒ４００”，”ｓｅｒｖｅｒ５００”…としておく。

【００８６】クライアントは、ＨＴＴＰプロトコルを用いて、以下のような第１のサービス要求メッセージ（ｓｅｒｖｉｃｅ１）を中継・監視サーバに送信する。

【００８７】

【数１】ＧＥＴ ／ｓｅｒｖｉｃｅ１ ＨＴＴＰ／１．

1

【００８８】中継・監視サーバ２は、第１のサービス要求メッセージを受信すると、これを要求メッセージ解析部２２０に渡す。

【００８９】要求メッセージ解析部２２０は、第１のサービス要求メッセージ中の要求パラメータとして”ｓｅｒｖｉｃｅ１”を抽出する。次いで、自身が持つＵＲＬ対応テーブルを検索して、”ｓｅｒｖｉｃｅ１”に対応するＵＲＬ”ｈｔｔｐ：／／ｓｅｒｖｅｒ３００／ｏｂｊｅｃｔ３１０”を取り出して、これを監査証生成部２１０に渡す。このＵＲＬは、ドメイン名”ｓｅｒｖｅｒ３００”を持つサーバ３のサービス・オブジェクト部が所有するサービス・オブジェクト”ｏｂｊｅｃｔ３１０”を要求するものとする。

【００９０】監査証生成部２１０は、メッセージの識別子、有効期限、サービス名の３項のパラメータからなる以下のようなデータを生成する。

【００９１】

【数２】

(1, 199806081010:199806081015, service1)

【００９２】上記の３項組のデータは、識別子が１、有効期限（但し世界時刻とする）が１９９８年６月８日１０時１０分から同日の１０時１５分まで、サービス名がｓｅｒｖｉｃｅ１であること、すなわち、識別子１を持つサービス要求に対しては１９９８年６月８日１０時１０分から同日１０時１５分までの間ｓｅｒｖｉｃｅ１へのアクセスが許可されていることを示している。この３項組のデータは、要するにサービス・オブジェクトに対するアクセス権限を意味する。ネットワーク・コンピューティング関連の技術分野ではアクセス権限は「ケーパビリティ（Ｃａｐａｂｉｌｉｔｙ）」とも呼ばれる。

【００９３】監査証生成部２１０は、この３項組のデータに対してメッセージ・ダイジェスト関数を適用し、自分が保持する公開鍵暗号系の秘密鍵ｓｅｃｒｅｙｋｅｙ１を用いて電子署名を行う。ここで付された署名は、後続のサーバ３において「監査証１０」の役割を果たすが、以下では”ｓｉｇｎａｔｕｒｅ１”と呼ぶことにする。

【００９４】監査証生成部２１０は、要求された”ｓｅｒｖｉｃｅ１”に対応するＵＲＬ”ｈｔｔｐ：／／ｓｅｒｖｅｒ３００／ｏｂｊｅｃｔ３１０”を基にして、サーバ３の送受信部３４０に対して以下のような第２のサービス要求メッセージを送信する。

【００９５】

【数３】

```
GET /object310 HTTP/1.1
Capability: (1, 199806081010:199806081015, service1)
Signature: signature1
```

【００９６】サーバ３の送受信部３４０は、第２のサービス要求メッセージを受け取ると、これを要求メッセージ解析部３３０に渡す。要求メッセージ解析部３３０は、これに応答して以下の工程を実行する。

【００９７】（１）　メッセージの先頭行からサービス・オブジェクトの名前を抽出して、該サービス・オブジェクトについての第１のリファレンスを得る。

（２）　ＨＴＴＰにおけるリクエスト・ヘッダのうち”Ｃａｐａｂｉｌｉｔｙ”というフィールド名に対応する値を抽出して、第１のケーパビリティとする。

（３）　ＨＴＴＰにおけるリクエスト・ヘッダのうち”Ｓｉｇｎａｔｕｒｅ”というフィールド名に対応する値を抽出して、第１の署名とする。

（４）　第１のケーパビリティに記述された有効期限が期限内かどうかを検査する。期限内であれば次工程に進むが、そうでなければ当該ケーパビリティが無効である旨の応答メッセージを送受信部３４０に入力する。

（５）　第１のケーパビリティが無効識別子テーブルの中に存在するかどうかを検索する。該テーブル中になければ次工程に進むが、そうでなければ当該ケーパビリティが無効である旨の応答メッセージを送受信部３４０に入力する。

（６）　中継・監視サーバ２の公開鍵を用いて、第１の署名が第１のケーパビリティの正しい署名であるかどうかを検査する。正しい署名であれば、第１のケーパビリティの識別子を無効識別子テーブルに追加する。

（７）　第１のリファレンスで示されるサービス・オブジェクト部３１０に要求メッセージを渡す。また、第１のケーパビリティと第１の署名を要求メッセージ生成部３６０に入力する。

【００９８】一度受理したケーパビリティの識別子を無効識別子テーブルに登録しておくことにより、ネットワーク上の不正者が同じケーパビリティを流用するのを防止することができる。

【００９９】第２のサービス要求メッセージに応答するために、さらにサーバ４が持つサービス・オブジェクトを必要とするときには、サーバ３のサービス・オブジェクト部３１０は、サーバ４のサービス・オブジェクト部４１０にサービス要求メッセージを送信すべく、要求メッセージ生成部３６０に要求メッセージの生成を要求する。

【０１００】要求メッセージ生成部３６０は、サーバ３自身が所持する公開鍵暗号系のｓｅｃｔｒｅｔｋｅｙ２を用いて第２の署名ｓｉｇｎａｔｕｒｅ２を作成し、第１のケーパビリティと第１の署名と第２の署名（すなわち「監査証２０」）を含んだ第３のサービス要求メッセージを生成する。

【０１０１】サーバ３は、サーバ４に対して、ＨＴＭＬファイル中のテーブルの後半部分を要求するものとする。この場合、第３のサービス要求メッセージは以下のようになる。

【０１０２】
【数４】
GET /object410 HTTP/1.1
Capability: (1, 199806081010:199806081015, service1)
Signature: signature1
Signature: signature2

【０１０３】サーバ４の要求メッセージ解析部４３０は、第３のサービス要求メッセージを受け取ると、以下の工程を実行する。

【０１０４】（１）　メッセージの先頭行からサービス・オブジェクトの名前を抽出して、サービス・オブジェクトの第２のリファレンスを得る。

（２）　ＨＴＴＰにおけるリクエスト・ヘッダの形式のうち”Ｃａｐａｂｉｌｉｔｙ”というフィールド名に対応する値を抽出して、第１のケーパビリティ（アクセス権限）とする。

（３）　ＨＴＴＰにおけるリクエスト・ヘッダの形式のうち”Ｓｉｇｎａｔｕｒｅ”というフィールド名に対応する値を抽出して、第１の署名とする。

（４）　ＨＴＴＰにおけるリクエスト・ヘッダの形式のうち”Ｓｉｇｎａｔｕｒｅ２”というフィールド名に対応する値を抽出して、第２の署名とする。

（５）　第１のケーパビリティの有効期限が期限内であるかどうかを検査する。期限内であれば次工程に進むが、そうでなければ該ケーパビリティが無効である旨の応答メッセージを送受信部４１０に渡す。

（６）　第１のケーパビリティの識別子が無効識別子テーブルの中にあるかどうかを検索する。該テーブル中になければ次工程に進むが、そうでなければ該ケーパビリティが無効である旨の応答メッセージを送受信部４１０に入力する。

（７）　第１の署名が第１のケーパビリティの正しい署名であるかどうかを、中継・監視サーバ２の公開鍵を用いて検査する。正しい署名であれば、第１のケーパビリティの識別子を無効識別子テーブルに追加する。

（８）　第２の署名が第１のケーパビリティの正しい署名であるかどうかを、サーバ３の公開鍵を用いて検査する。正しい署名であれば次工程に進むが、そうでなければ工程を中止する。

（９）　第１のリファレンスで示されるサービス・オブジェクト部４１０に要求メッセージを渡す。また、第１のケーパビリティと第１の署名を要求メッセージ生成部４６０に入力する。

【０１０５】一度受理したケーパビリティの識別子を無効識別子テーブルに登録しておくことにより、ネットワーク上の不正者が同じケーパビリティを流用するのを防止することができる。

【０１０６】要求メッセージを受け取ったサービス・オブジェクト部４１０は、要求されたＨＴＭＬファイル中のテーブルの後半部分を生成する。サービス・オブジェクト部４１０が提供するサービス・オブジェクトの実体は、例えば以下のようなものである。

【０１０７】
【数５】
＜ｔｒ＞
＜ｔｄ＞　ｂｂｂｂ１００
＜ｔｄ＞　１００
＜ｔｄ＞　１０００
＜ｔｒ＞
＜ｔｄ＞　ｂｂｂｂ２００
＜ｔｄ＞　２００
＜ｔｄ＞　２０００
＜ｔｒ＞
＜ｔｄ＞　ｂｂｂｂ３００
＜ｔｄ＞　３００
＜ｔｄ＞　３０００

【０１０８】サービス・オブジェクト部４１０は、このような「文書１」を生成して、応答メッセージ生成部４２０に渡す。

【０１０９】応答メッセージ生成部４２０は、サーバ４が所持する公開鍵暗号系の秘密鍵を用いて文書１に署名を施すことでサービス応答メッセージを生成する。そして、送受信部４４０を介してサーバ３の送受信部３４０にサービス応答メッセージを送信する。サービス応答メッセージに付された署名は「受領証３０」としての意味を持つ。

【０１１０】サーバ３の送受信部３４０は、サービス応答メッセージを受け取ると、これを応答メッセージ解析部３５０に渡す。

【０１１１】応答メッセージ解析部３５０は、サービス応答メッセージを解析し、サーバ４の公開鍵を用いて署名の認証を行う。この認証作業は、サーバ３が自分の子孫にあたる各サーバ４，５，６に対する認証局としての役割も持つことを意味する。

【０１１２】署名が正しく認証されたならば、応答メッセージ解析部３５０はサービス応答メッセージ中の文書１をサービス・オブジェクト部３１０に渡す。

【０１１３】サービス・オブジェクト部３１０は、要求されたＨＴＭＬファイル中のテーブルの前半部分を生成する。サービス・オブジェクト部４１０が提供するサービス・オブジェクトの実体は、例えば以下に示すような「文書２」である。

【０１１４】
【数６】
＜ｔｒ＞
＜ｔｄ＞　ａａａａ１００
＜ｔｄ＞　１００
＜ｔｄ＞　１０００
＜ｔｒ＞

＜ｔｄ＞　ａａａａ２００
＜ｔｄ＞　２００
＜ｔｄ＞　２０００
＜ｔｒ＞
＜ｔｄ＞　ａａａａ３００
＜ｔｄ＞　３００
＜ｔｄ＞　３０００

【０１１５】サービス・オブジェクト部３１０は、上述の文書１と文書２とを連結して「文以下に示すような「文書３」を生成する。

【０１１６】

【数７】

＜ｈｔｍｌ＞
＜ｈｅａｄ＞
＜ｔｉｔｌｅ＞表の合成結果＜／ｔｉｔｌｅ＞
＜／ｈｅａｄ＞
＜ｂｏｄｙ＞
＜ｔａｂｌｅ＞
＜ｔｒ＞
＜ｔｄ＞　ａａａａ１００
＜ｔｄ＞　１００
＜ｔｄ＞　１０００
＜ｔｒ＞
＜ｔｄ＞　ａａａａ２００
＜ｔｄ＞　２００
＜ｔｄ＞　２０００
＜ｔｒ＞
＜ｔｄ＞　ａａａａ３００
＜ｔｄ＞　３００
＜ｔｄ＞　３０００
＜ｔｒ＞
＜ｔｄ＞　ｂｂｂｂ１００
＜ｔｄ＞　１００
＜ｔｄ＞　１０００
＜ｔｒ＞
＜ｔｄ＞　ｂｂｂｂ２００
＜ｔｄ＞　２００
＜ｔｄ＞　２０００
＜ｔｒ＞
＜ｔｄ＞　ｂｂｂｂ３００
＜ｔｄ＞　３００
＜ｔｄ＞　３０００
＜／ｔａｂｌｅ＞
＜／ｂｏｄｙ＞
＜／ｈｔｍｌ＞

【０１１７】生成された文書３は、応答メッセージ生成部３２０に渡される。

【０１１８】応答メッセージ生成部３２０は、サーバ３が所持する公開鍵暗号系の秘密鍵を用いて文書３に署名を行い、サービス応答メッセージを生成する。サービス

応答メッセージに付された署名は、「受領証８０」としての意味を持つ。そして、サービス応答メッセージは、送受信部３４０を介して中継・監査サーバ２の送受信部２４０に送信される。

【０１１９】中継・監視サーバ２の送受信部２４０は、受け取ったサービス応答メッセージを応答メッセージ解析部２５０に渡す。

【０１２０】応答メッセージ解析部２５０は、サーバ３及びサーバ４の各々の公開鍵を用いて監査証８０に含まれる各署名を検査する。すなわち、中継・監視サーバ２は、サービスを提供する各サーバ３，４…に対する認証局として機能する。

【０１２１】正しく認証されたときには、文書３は送受信部２４０を介してクライアント１に送信されるが、認証に失敗したときには、文書３に代わって、サービス応答メッセージが正しくない旨の応答メッセージを送信する。

【０１２２】なお、上記の説明では、クライアント１からのサービス要求に対して、サーバ３はサーバ４とのみ連携して応答する例を挙げたが、サーバ３がサーバ５及びサーバ６と連携する場合も同様である。このような場合、サーバ３がサーバ５に要求メッセージを送信するときには「監査証４０」が、サーバ５がサーバ６に要求メッセージを送信するときには「監査証５０」が、夫々添付される。また、サーバ６がサーバ５に応答メッセージを送信するときには「受領証６０」が、サーバ５がサーバ３に応答メッセージを送信するときには「受領証７０」が、夫々添付される。

【０１２３】また、上述の実施例では、ネットワークを介してコンピュータ同士がメッセージを送受するためのプロトコルとしてＨＴＴＰを取り上げたが、他の任意のプロトコルを使用しても同様に本発明を適用することができる。プロトコルは、例えば、ＨＴＴＰＳ，Ｓ－ＨＴＴＰ（ｓｅｃｕｒｅ　ＨＴＴＰ），ＦＴＰ（ＦｉｌｅＴｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ），ＣＯＲＢＡ（Ｃｏｍｍｏｎ　ＯＲＢＡｒｃｈｉｔｅｃｔｕｒｅ），ＩＩＯＰ（Ｉｎｔｅｒｎｅｔ　Ｉｎｔｅｒ－ＯＲＢ　Ｐｒｏｔｏｃｏｌ），ＪａｖａＲＭＩ（Ｒｅｍｏｔｅ　Ｍｅｔｈｏｄ　Ｉｎｖｏｃａｔｉｏｎ）のいずれであってもよい。

【０１２４】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１２５】

【発明の効果】以上詳記したように、本発明によれば、

１以上のサーバと１以上のクライアントからなる分散型のネットワーク・システムにおいてクライアントがサーバに対してサービスを要求するための、優れた遠隔手続き呼び出しを行う方式を提供することができる。

【０１２６】また、本発明によれば、少なくとも１つの中継・監査サーバを中継してサービスの要求がサーバに届くようなタイプの、優れた遠隔手続き呼び出し方式を提供することができる。

【０１２７】また、本発明によれば、複数のサーバの協働的な動作によってクライアントから要求されたサービスを提供するような分散型のネットワーク環境において、サービスの正当な履行を保証するための優れた方式を提供することができる。

【０１２８】また、本発明によれば、ネットワーク上に中継・監査サーバを配設することで、サービス要求の出所を認証したり、サーバから提供されたサービスを保証することができる、優れた遠隔手続き／メソッド呼び出し方式を提供することができる。

【図面の簡単な説明】

【図１】　本発明の実施に供されるネットワーク・システム１００の構成を模式的に示した図である。

【図２】　クライアントからのあるサービスを提供するために形成されたサーバの木構造を模式的に示した図である。

【図３】　本発明を実現する中継・監視サーバ２の構成を模式的に示したブロック図である。

【図４】　本発明の実施に供されるサーバ３の構成を模式的に示したブロック図である。

【図５】　ネットワーク・システム１００上において遠隔手続き呼び出しを処理するためのオペレーションを模式的に示した図である。

【図６】　ネットワーク上で、WWWサーバがデータベース・サーバと協調してクライアントから呼び出された遠隔手続きを処理する様子を模式的に示した図である。

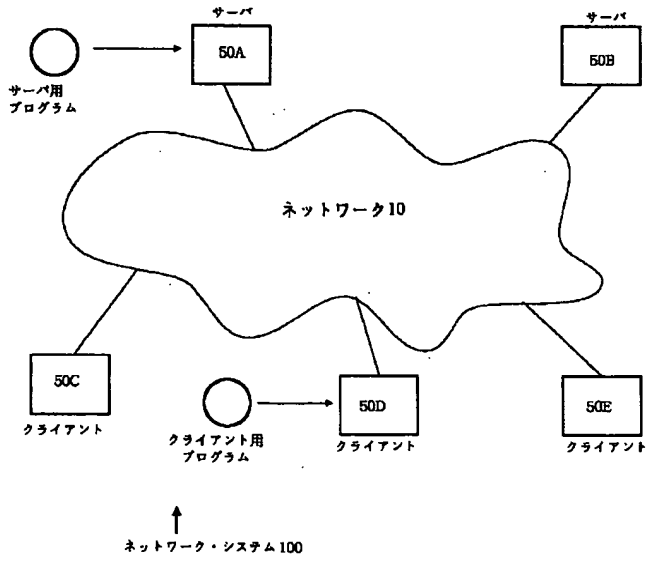
【図７】　ネットワーク上において、多数のサーバが連携してクライアントのサービス要求に応答する様子を模式的に示した図であり、より具体的には、多数のサーバはサービス要求／応答に関する木構造を形成し、且つ、各サーバは互いに異なる組織に属している様子を示した図である。

【図８】　ネットワーク上において、多数のサーバが連携してクライアントのサービス要求に応答する様子を模式的に示した図であり、より具体的には、一部の子サーバがダミーのクライアントを用いて不正なサービス要求を発行する様子を示した図である。

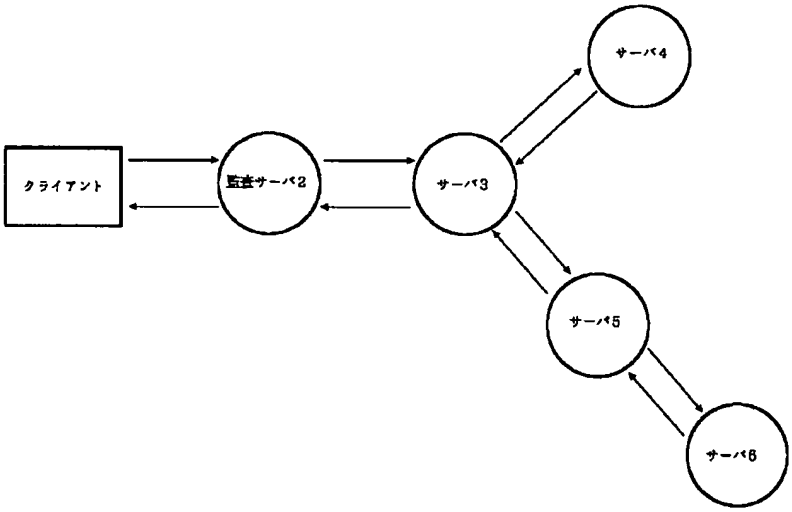
【符号の説明】

１００…ネットワーク・システム
２１０…監査証生成部
２２０…要求メッセージ解析部
２３０…送受信部
２４０…応答メッセージ解析部
２５０…受領証生成部

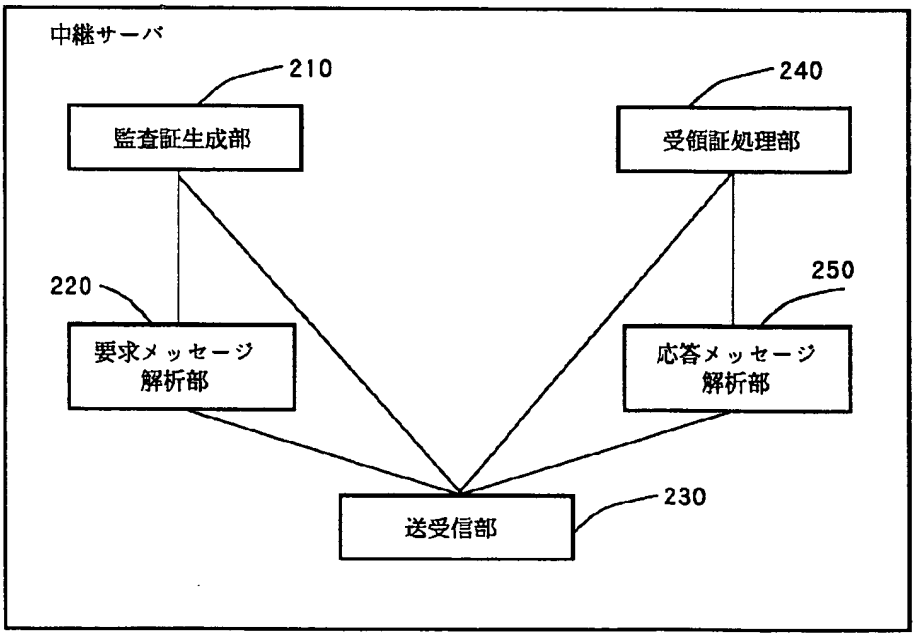
【図１】



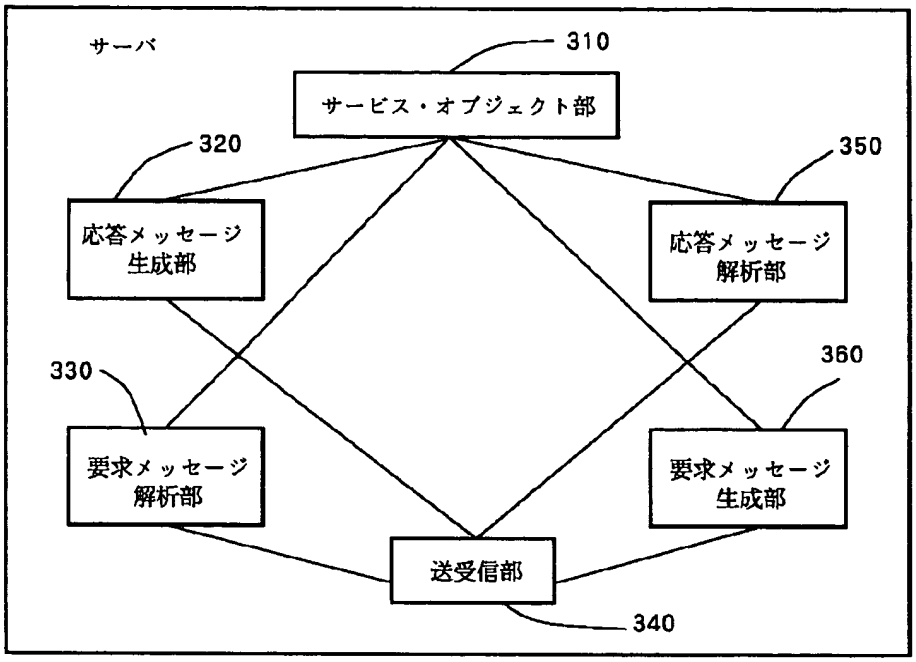
【図２】


クライアント
監査サーバ2
サーバ3
サーバ4
サーバ5
サーバ6

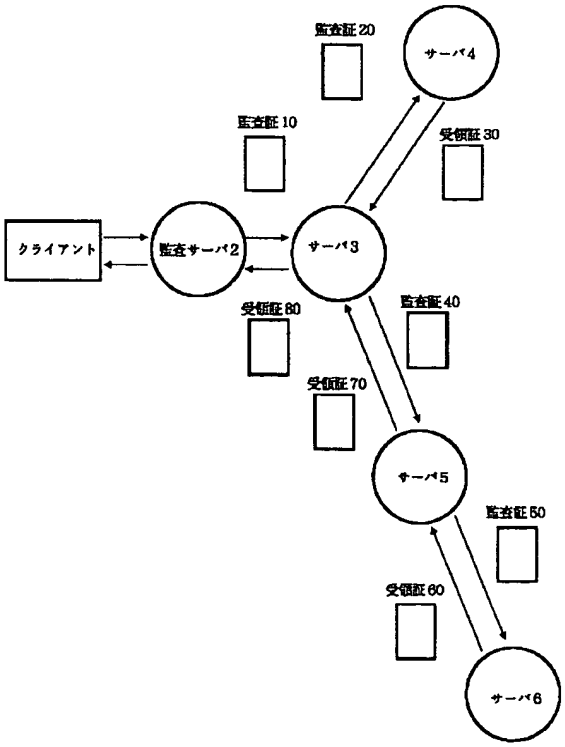
【図３】


中継サーバ
210
監査証生成部
240
受領証処理部
220
要求メッセージ
解析部
250
応答メッセージ
解析部
230
送受信部

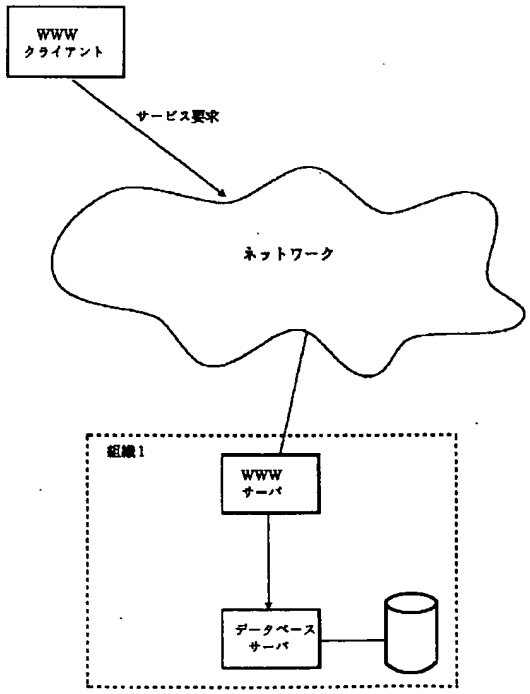
【図４】


サーバ
310
サービス・オブジェクト部
320
350
応答メッセージ
生成部
応答メッセージ
解析部
330
360
要求メッセージ
解析部
要求メッセージ
生成部
送受信部
340

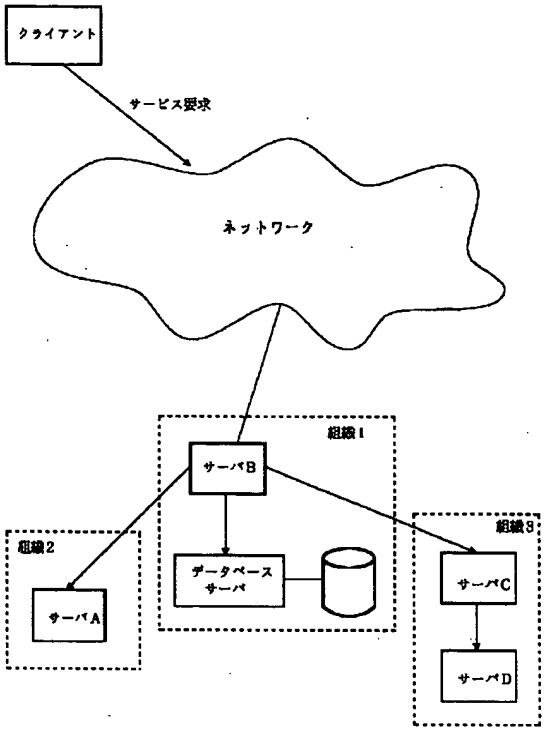
【図５】


監査証20
サーバ4
監査証10
受領証30
クライアント
監査サーバ2
サーバ3
受領証80
監査証40
受領証70
サーバ5
監査証50
受領証60
サーバ6

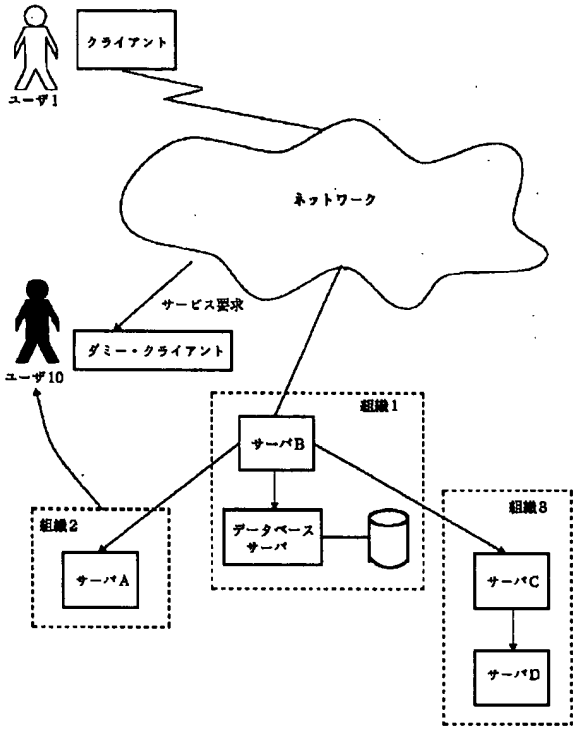
【図６】


WWW
クライアント
サービス要求
ネットワーク
組織1
WWW
サーバ
データベース
サーバ

【図７】


クライアント
サービス要求
ネットワーク
組織1
サーバB
組織2
サーバA
データベース
サーバ
組織3
サーバC
サーバD

【図８】


クライアント
ユーザ1
ネットワーク
サービス要求
ダミー・クライアント
ユーザ10
組織1
サーバB
組織2
サーバA
データベース
サーバ
組織3
サーバC
サーバD

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.